PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-306001
(43)Date of publication of application : 02.11.2000

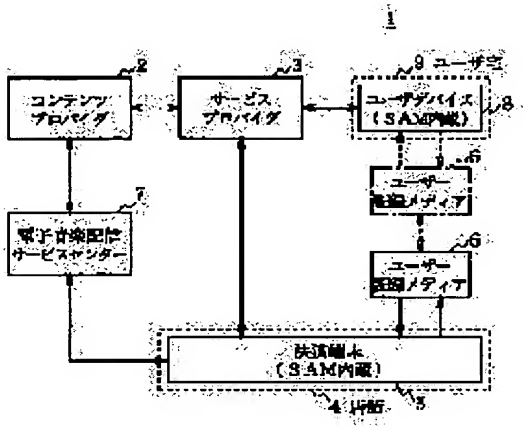
(51)Int.Cl. G06F 17/60
G09C 1/00
G11B 20/10
H04L 9/32
// G06F 19/00

(21)Application number : 11-118618
(22)Date of filing : 26.04.1999

(71)Applicant : SONY CORP
(72)Inventor : NAGAI KIKO

(54) DEVICE, METHOD, AND SYSTEM FOR DATA SETTLEMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To easily settle supplied provision data without any complicated procedure or operation by receiving money from a user and settling the account when a user device is authenticated according to user identification information.
SOLUTION: An electronic music distribution service center 7 decides that a user device 8 is already registered in the center 7 according to a specific public key. A settlement terminal 5 displays a music name of digital music contents and the value of its purchase on a monitor according to service condition information and charging information read out of its storage module. On the screen, a user selects the digital music contents and its value of the selected digital music contents is paid in cash or with a prepaid card or cash card through a prescribed throw-in hole. The settlement terminal 5 displays that on the monitor to inform the user.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－306001
（P2000－306001A）
(43)公開日　平成12年11月２日(2000.11.2)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	３３０	５Ｂ０４９
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｂ	５Ｂ０５５
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｄ０４４
Ｈ０４Ｌ　9/32		Ｇ０６Ｆ　15/21	Ｚ	５Ｊ１０４
// Ｇ０６Ｆ　19/00		Ｈ０４Ｌ　9/00	６７３Ｅ	

審査請求　未請求　請求項の数18　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平11－118618

(22)出願日　平成11年４月26日(1999.4.26)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　永井　規浩
東京都品川区北品川６丁目７番35号ソニー株式会社内
(74)代理人　100082740
弁理士　田辺　恵基

最終頁に続く

(54)【発明の名称】　データ決済装置、データ決済方法及びデータ決済システム

(57)【要約】
【課題】本発明は、供給される提供データの決済を煩雑な手続きや操作なしに容易に実行し得る。
【解決手段】本発明は、所定の記録媒体に対して記録及び又は再生を行うユーザ機器を特定するユーザ識別情報を記録媒体から読み取り、当該読み取られたユーザ識別情報に基づいてユーザ機器を認証し、当該ユーザ機器を認証したとき、ユーザに選択された所望の提供データの供給条件に対応した対価の入金をユーザから受けて決済を行うようにする。

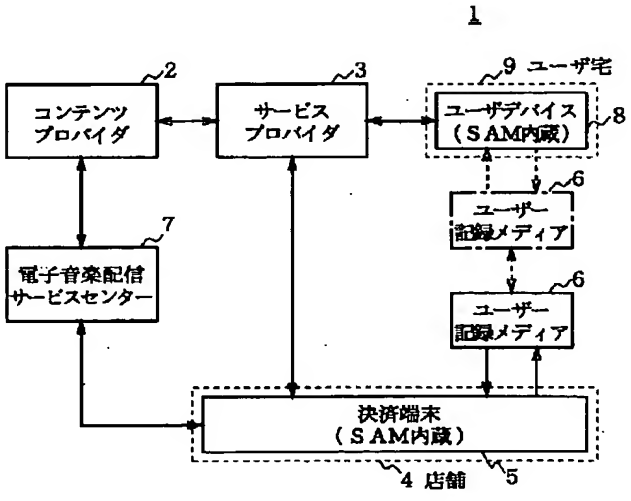


図１　電子音楽配信システムの全体構成

【特許請求の範囲】
【請求項１】所定の記録媒体に対して記録及び又は再生を行うユーザ機器を特定するユーザ識別情報を上記記録媒体から読み取る読取手段と、
上記読取手段によって読み取られた上記ユーザ識別情報に基づいて上記ユーザ機器を認証する認証手段と、
上記認証手段によって上記ユーザ機器を認証したとき、ユーザに選択された所望の提供データの供給条件に対応した対価の入金を上記ユーザから受けて決済を行う決済手段とを具えることを特徴とするデータ決済装置。
【請求項２】上記データ決済装置は、
上記認証手段によって上記ユーザ機器を認証したとき、上記提供データを上記記録媒体に記録するデータ記録手段を具えることを特徴とする請求項１に記載のデータ決済装置。
【請求項３】上記データ記録手段は、上記提供データを所定の方式で暗号化した後に上記記録媒体に記録することを特徴とする請求項２に記載のデータ決済装置。
【請求項４】上記データ決済装置は、
上記提供データの供給条件に応じた販売履歴を所定の送信先へ送信する送信手段を具えることを特徴とする請求項１に記載のデータ決済装置。
【請求項５】上記決済手段は、
上記認証手段によって上記ユーザを認証したとき、上記ユーザ機器と所定のデータ配信装置とがオンライン接続された状態で、上記データ配信装置から供給されて上記記録媒体に記録された上記提供データの再生履歴を上記供給条件として上記読取手段によって読み取り、上記再生履歴に基づいて上記提供データの再生回数に対応した上記対価の金額を所定の表示部に表示した後、上記金額の入金を受けて上記決済を行うことを特徴とする請求項１に記載のデータ決済装置。
【請求項６】上記決済手段は、上記提供データの再生回数に対応した上記対価を決済した後に上記記録媒体から上記再生履歴を削除することを特徴とする請求項５に記載のデータ決済装置。
【請求項７】所定の記録媒体に対して記録及び又は再生を行うユーザ機器を特定するユーザ識別情報を上記記録媒体から読み取る読取ステップと、
上記読取ステップで読み取られた上記ユーザ識別情報に基づいて上記ユーザ機器を認証する認証ステップと、
上記認証ステップで上記ユーザ機器を認証したとき、ユーザに選択された所望の提供データの供給条件に対応した対価の入金を上記ユーザから受けて決済を行う決済ステップとを具えることを特徴とするデータ決済方法。
【請求項８】上記データ決済方法は、
上記認証ステップで上記ユーザ機器を認証したとき、上記提供データを上記記録媒体に記録するデータ記録ステップを具えることを特徴とする請求項７に記載のデータ決済方法。
【請求項９】上記データ記録ステップは、上記提供データを所定の方式で暗号化した後に上記記録媒体に記録することを特徴とする請求項８に記載のデータ決済方法。
【請求項１０】上記データ決済方法は、
上記決済ステップに続いて、上記提供データの供給条件に応じた販売履歴を所定の送信先へ送信する送信ステップを具えることを特徴とする請求項７に記載のデータ決済方法。
【請求項１１】上記決済ステップは、
上記認証ステップによって上記ユーザを認証したとき、上記ユーザ機器と所定のデータ配信装置とがオンライン接続された状態で、上記データ配信装置から供給されて上記記録媒体に記録された上記提供データの再生履歴を上記供給条件として上記読取ステップで読み取り、上記再生履歴に基づいて上記提供データの再生回数に対応した上記対価の金額を所定の表示部に表示した後、上記金額の入金を受けて上記決済を行うことを特徴とする請求項７に記載のデータ決済方法。
【請求項１２】上記決済ステップは、上記提供データの再生回数に対応した上記対価を決済した後に上記記録媒体から上記再生履歴を削除することを特徴とする請求項１１に記載のデータ決済方法。
【請求項１３】提供データを生成して提供するデータ提供装置、当該データ提供装置から供給された上記提供データを配信するデータ配信装置、当該データ配信装置によって配信された上記提供データの供給条件に対応した対価の入金を受けて決済を行うデータ決済装置、上記データ提供装置と上記データ配信装置と上記データ決済装置とを管理するデータ管理装置からなるデータ決済システムにおいて、
上記データ決済装置は、
所定の記録媒体に対して記録及び又は再生を行うユーザ機器を特定するユーザ識別情報を上記記録媒体から読み取る読取手段と、
上記読取手段によって読み取られた上記ユーザ識別情報に基づいて上記ユーザ機器を認証する認証手段と、
上記認証手段によって上記ユーザ機器を認証したとき、ユーザに選択された所望の上記提供データの上記供給条件に対応した上記対価の入金を上記ユーザから受けて決済を行う決済手段とを具えることを特徴とするデータ決済システム。
【請求項１４】上記データ決済装置は、
上記認証手段によって上記ユーザ機器を認証したとき、上記提供データを上記記録媒体に記録するデータ記録手段を具えることを特徴とする請求項１３に記載のデータ決済システム。
【請求項１５】上記データ記録手段は、上記提供データを所定の方式で暗号化した後に上記記録媒体に記録することを特徴とする請求項１４に記載のデータ決済システム。

【請求項１６】上記データ決済装置は、
上記提供データの供給条件に応じた販売履歴を上記データ管理装置へ送信する送信手段を具えることを特徴とする請求項１３に記載のデータ決済システム。
【請求項１７】上記データ決済装置の上記決済手段は、上記認証手段によって上記ユーザを認証したとき、上記ユーザ機器と上記データ配信装置とがオンライン接続された状態で、上記データ配信装置から供給されて上記記録媒体に記録された上記提供データの再生履歴を上記供給条件として上記読取手段によって読み取り、上記再生履歴に基づいて上記提供データの再生回数に対応した上記対価の金額を所定の表示部に表示した後、上記金額の入金を受けて上記決済を行うことを特徴とする請求項１３に記載のデータ決済システム。
【請求項１８】上記データ決済装置の上記決済手段は、上記提供データの再生回数に対応した上記対価を決済した後に上記記録媒体から上記再生履歴を削除することを特徴とする請求項１７に記載のデータ決済システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はデータ決済装置、データ決済方法及びデータ決済システムに関し、例えば所望のディジタルコンテンツの決済を行うデータ決済装置、データ決済方法及びデータ決済システムに適用して好適なものである。
【０００２】
【従来の技術】近年、インターネットによるコンピュータネットワークを用いて映画や音楽等のディジタルコンテンツを配信する情報提供サービスが始まっている。このような情報提供サービスの中で例えば電子音楽配信システムにおいては、レコード会社のようなコンテンツプロバイダによって作成されたディジタル音楽コンテンツを所定のサービスプロバイダからインターネット等のネットワークを介してオンラインでユーザ宅へ配信するようになされている。
【０００３】ユーザ宅では、パーソナルコンピュータ等のユーザ機器によって受信したディジタル音楽コンテンツをユーザが選定したサービス条件（例えば買い切り又は再生可能回数等）の基で再生し、当該サービス条件の基で利用したコンテンツ利用履歴をユーザログとして記憶し、これを電子音楽配信サービスセンタへ送信する。
【０００４】電子音楽配信サービスセンタは、送られてきたユーザログに基づいて利用料金を算出し、この利用料金をユーザに通知することにより、利用料金を例えばユーザの銀行口座上で決済するようになされている。
【０００５】
【発明が解決しようとする課題】ところでかかる構成の電子音楽配信システムにおいて、電子音楽配信サービスセンタが利用料金を銀行口座上で決済するためには、予めユーザのクレジットカード番号や銀行口座番号を予め保持しておく必要がある。
【０００６】従ってユーザは、ディジタル音楽コンテンツの配信を受けてその決済を行うために、クレジットカート番号や銀行口座番号をオンラインで電子音楽配信サービスセンタに送信するといった面倒な手続きを要する問題があった。
【０００７】また電子音楽配信システムにおいては、電子音楽配信サービスセンタに直接オンラインで接続し得る機器をユーザが所有していなければ、ディジタル音楽コンテンツの配信を受けることができず、誰でもが容易にディジタル音楽コンテンツの入手及び決済を実行し得ないという問題があった。
【０００８】本発明は以上の点を考慮してなされたもので、供給される提供データの決済を煩雑な手続きや操作なしに容易に実行し得るデータ決済装置、データ決済方法及びデータ決済システムを提案しようとするものである。
【０００９】
【課題を解決するための手段】かかる課題を解決するため本発明のデータ決済装置及びデータ決済方法においては、所定の記録媒体に対して記録及び又は再生を行うユーザ機器を特定するユーザ識別情報を記録媒体から読み取り、当該読み取られたユーザ識別情報に基づいてユーザ機器を認証し、当該ユーザ機器を認証したとき、ユーザに選択された所望の提供データの供給条件に対応した対価の入金をユーザから受けて決済を行うようにする。
【００１０】データ決済装置及びデータ決済方法では、記録媒体から読み取ったユーザ識別情報を基にユーザ機器を認証し得た場合に限って、ユーザに選択された提供データの供給条件に対応した対価の入金を受け付けて決済を行うようにしたことにより、認証し得た特定のユーザに対して支払いを行うための個人データの煩雑な入力手続きを強いることなく提供データの決済を行うことができる。
【００１１】また本発明のデータ決済システムにおいては、提供データを生成して提供するデータ提供装置、当該データ提供装置から供給された提供データを配信するデータ配信装置、当該データ配信装置によって配信された提供データの供給条件に対応した対価の入金を受けて決済を行うデータ決済装置、データ提供装置とデータ配信装置とデータ決済装置を管理するデータ管理装置からなるデータ決済システムにおいて、データ決済装置は、所定の記録媒体に対して記録及び又は再生を行うユーザ機器を特定するユーザ識別情報を上記記録媒体から読み取る読取手段と、当該読取手段によって読み取られたユーザ識別情報に基づいてユーザ機器を認証する認証手段と、当該認証手段によってユーザ機器を認証したとき、ユーザに選択された所望の提供データの供給条件に対応した対価の入金をユーザから受けて決済を行う決済手段とを設ける。

【００１２】データ決済システムでは、データ決済装置によって記録媒体から読み取ったユーザ識別情報を基にユーザ機器を認証し得た場合に限って、データ配信装置から配信されてユーザに選択された提供データの供給条件に対応した対価の入金を受け付けて決済を行うようにしたことにより、認証し得た特定のユーザに対して支払いを行うための個人データの煩雑な入力手続きを強いることなく提供データの決済を行うことができる。

【００１３】

【発明の実施の形態】以下図面について、本発明の一実施の形態を詳述する。

【００１４】（１）電子音楽配信システムの全体構成

図１において、１は全体として本発明によるデータ決済システムとしての電子音楽配信システムを示し、ユーザに提供されるコンテンツとしては情報そのものが価値を有するディジタル音楽データを一例として以下説明を行う。

【００１５】電子音楽配信システム１は、提供データとしてのディジタル音楽コンテンツを作成するデータ提供装置としてのコンテンツプロバイダ２と、当該コンテンツプロバイダ２によって作成されたディジタル音楽コンテンツを配信するデータ配信装置としてのサービスプロバイダ３と、当該サービスプロバイダ３から供給されたディジタル音楽コンテンツをフラッシュメモリカードでなるユーザ記録メディア６に書き込むと共に、その対価の支払いを受けて決済を行う店舗４に設置されたデータ決済装置としての決済端末５と、これら一連のディジタル音楽コンテンツの配信や決済に関する種々の管理を行うデータ管理装置としての電子音楽配信サービスセンタ７とから構成されている。

【００１６】また電子音楽配信システム１は、サービスプロバイダ３とユーザ宅９に設置されている例えばパーソナルコンピュータ等のユーザデバイス８とをインターネット等のネットワーク（図示せず）を介してオンライン接続し、サービスプロバイダ３から供給されるディジタル音楽コンテンツをユーザ機器としてのユーザデバイス８を介してユーザ記録メディア６にダウンロードし得るようにもなされている。

【００１７】（１－１）コンテンツプロバイダの構成

コンテンツプロバイダ２は、図２に示すようにコンテンツサーバ１１に記憶しているユーザ供給用のディジタル音楽コンテンツＤ１１を圧縮部１２に送出する。圧縮部１２は、例えばＡＴＲＡＣ２(Adaptive Transform Acoustic Coding 2)（商標）と呼ばれる高能率符号化方式でディジタル音楽コンテンツＤ１１を圧縮符号化し、これをディジタル音楽コンテンツＤ１２として第１暗号化部１３に送出する。

【００１８】第１暗号化部１３は、圧縮符号化されたディジタル音楽コンテンツＤ１２に対して乱数発生部１４から供給された所定ビット数の乱数をコンテンツキーＫcoとして用いてＤＥＳ(Data Encryption Standard)等の共通鍵暗号方式で暗号化し、これをコンテンツキーＫcoによって暗号化されたディジタル音楽コンテンツＤ１３としてセキュアコンテナ作成部１７に送出する。

【００１９】第２暗号化部１５は、第１暗号化部１３と同様に乱数発生部１４からコンテンツキーＫcoの供給を受け、電子音楽配信センタ７から供給された配送用キーＫdを用いてコンテンツキーＫcoをＤＥＳ等の共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部１７に送出する。

【００２０】ポリシー記憶部１６は、第１暗号化部１３から供給されたディジタル音楽コンテンツＤ１３の取扱方針（ポリシー）を記憶しており、ディジタル音楽コンテンツＤ１３に対応した取扱方針をセキュアコンテナ作成部１７に送出する。

【００２１】セキュアコンテナ作成部１７は、図３に示すようにコンテンツキーＫcoによって暗号化されたディジタル音楽コンテンツＤ１３、配送用キーＫd によって暗号化されたコンテンツキーＫco、取扱方針、コンテンツキーＫcoで暗号化されたディジタル音楽コンテンツＤ１３と暗号化されたコンテンツキーＫcoと取扱方針とのハッシュ値に基づいて作成されたディジタル署名により構成されるコンテンツプロバイダセキュアコンテナＤ１４を生成し、これをサービスプロバイダ３へ供給する。

【００２２】相互認証部１８は、電子音楽配信サービスセンタ７から配送用キーＫd の供給を受けるのに先立って、ディジタル署名を用いて電子音楽配信サービスセンタ７と相互認証し、またサービスプロバイダ３へのコンテンツプロバイダセキュアコンテナＤ１４の供給に先立って、ディジタル署名を用いてサービスプロバイダ３と相互認証する。

【００２３】従って第２暗号化部１５は、相互認証部１８によって電子音楽配信サービスセンタ７との間で相互認証が得られると、電子音楽配信サービスセンタ７から配送用キーＫd の供給を受ける。またセキュアコンテナ作成部１７は、相互認証部１８によってサービスプロバイダ３との間で相互認証が得られると、コンテンツプロバイダセキュアコンテナＤ１４をサービスプロバイダ３へ供給する。

【００２４】なおディジタル署名とは、送信者が例えば所定のメッセージを受信者に対して送信したとき、受信者の受け取ったメッセージが本当に送信者から送られてきたものなのか、あるいは送られてきたメッセージが何者かによって改ざんされていないか、という２つのことを確認し得るデータのことであり、送信すべきデータを基にハッシュ関数でハッシュ値をとり、これをコンテンツプロバイダ２における公開鍵暗号の秘密鍵Ｋscp で暗号化することにより作成される。

【００２５】ハッシュ関数は、送信すべき所定のデータを入力として所定ビット長のデータに圧縮し、これをハ

ッシュ値として出力する関数である。このハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したときにハッシュ値の多くのビットが変化し、また同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有している。

【００２６】ディジタル署名と送信されたデータを受信した受信者は、ディジタル署名を公開鍵暗号の公開鍵で復号してハッシュ値を得、さらに受信したデータのハッシュ値を算出して、当該算出したハッシュ値と公開鍵で復号したハッシュ値とを比較して等しいか否かを判定する。

【００２７】このとき両者のハッシュ値が等しいと判定されたときには、受信したデータが改ざんされておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されてきたデータであることがわかる。なおディジタル署名のハッシュ関数としては、例えばＳＨＡ(Secure Hash Standard)－１が用いられる。

【００２８】続いて、公開鍵暗号について具体的に説明

$$ed = 1 \mod L$$

【００３２】が成立し、ｄはユークリッドの互除法で算出できる。このときｎとｅとが公開鍵とされ、ｐ、ｑ及びｄが秘密鍵とされる。

$$C = M^e \mod n$$

【００３５】を用いた処理によって算出される。

【００３６】また暗号文Ｃは、次式

$$M = C^d \mod n$$

【００３８】を用いた処理によって平文Ｍに復号される。

【００３９】ここで証明については省略するが、ＲＳＡ暗号で平文を暗号文に変換し、これを復号できるのは、

$$M = C^d = (M^e)^d = M^{(ed)} \mod n \quad \cdots\cdots (4)$$

【００４１】が成立するからである。

【００４２】秘密鍵ｐとｑを知っているならば、公開鍵ｅから秘密鍵ｄを算出することはできるが、公開鍵ｎの素因数分解が計算量的に困難な程度に公開鍵ｎの桁数を大きくすれば、公開鍵ｎを知るだけでは公開鍵ｅから秘密鍵ｄを算出することはできないので復号できない。以上のようにＲＳＡ暗号では、暗号化に使用する場合の鍵

$$y^2 = x^3 + ax + b$$

【００４５】で示される楕円曲線上のある点をＢとし、楕円曲線上の点Ｂがｎ回加算されたときの加算結果をｎＢと定義する共に、楕円曲線上の点Ｂがｎ回減算されたときの加算結果についても定義する。

【００４６】この場合、ＢとｎＢとからｎを算出することは困難であることが証明されている。ＢとｎＢとを公開鍵としてｎを秘密鍵とした場合、暗号文C_1及びC_2は乱数ｒを用いて平文Ｍから公開鍵で次式

【００４７】

【数６】

$$C_1 = M + r\,n\,B \quad \cdots\cdots (6)$$

する。暗号化及び復号で同一の共通鍵を使用する共通鍵暗号方式に対して、公開鍵暗号方式は暗号化に使用する鍵と復号するときの鍵とがそれぞれ異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開してよい鍵は公開鍵と称され他方の秘密に保つ鍵は秘密鍵と称される。

【００２９】このような公開鍵暗号の中で代表的なＲＳＡ(Rivest-Shamir-Adleman) 暗号を説明すると、まず２つの十分に大きな素数であるｐ及びｑを求め、さらにｐとｑの積であるｎを求める。そして（ｐ－１）と（ｑ－１）の最小公倍数Ｌを算出し、さらに３以上Ｌ未満でかつＬと互いに素な数ｅを求める（すなわちｅとＬを共通に割り切れる数は、１のみである）。

【００３０】次に、Ｌを法とする乗算に関するｅの乗法逆元ｄを求める。すなわちｄ、ｅ及びＬとの間には、次式

【００３１】

【数１】

$$\cdots\cdots (1)$$

【００３３】暗号文Ｃは、平文Ｍから次式

【００３４】

【数２】

$$\cdots\cdots (2)$$

【００３７】

【数３】

$$\cdots\cdots (3)$$

フェルマーの小定理に根拠をおいており、次式

【００４０】

【数４】

と復号する場合の鍵とを異なる鍵に設定することができる。

【００４３】また、公開鍵暗号の他の例である楕円曲線暗号についても簡単に説明する。次式

【００４４】

【数５】

$$\cdots\cdots (5)$$

【００４８】

$$C_2 = rB$$

【００４９】を用いた処理によって算出される。

【００５０】また暗号文C_1及びC_2は、次式

$$M = C_1 - nC_2$$

【００５２】を用いた処理によって平文Mに復号される。

【００５３】このように復号できるのは、秘密鍵ｎを有するものだけであり、以上のようにＲＳＡ暗号と同様に楕円曲線暗号でも暗号化に使用する場合の鍵と復号する場合の鍵とを異なる鍵に設定することができる。

【００５４】（１－２）サービスプロバイダの構成

サービスプロバイダ３は、図４に示すようにコンテンツプロバイダ２から供給されたコンテンツプロバイダセキュアコンテナＤ１４のうちコンテンツキーKcoで暗号化されたディジタル音楽コンテンツＤ１３をコンテンツサーバ２１に記憶した後、これをセキュアコンテナ作成部２５に送出する。ここでコンテンツキーKcoは、配送用キーKd によって暗号化されている状態である。

【００５５】サービスプロバイダ３の値付け部２２は、コンテンツプロバイダセキュアコンテナＤ１４に含まれる取扱方針を基にディジタル音楽コンテンツＤ１３に対するサービス条件（買い切り又は再生可能回数）に応じた価格情報を作成し、これをセキュアコンテナ作成部２５に送出する。

【００５６】因みにサービス条件の買い取りとは、ユーザ記録メディア６に記録されたディジタル音楽コンテンツＤ１３をユーザ宅９のユーザデバイス８によって何度でも再生し得るディジタル音楽コンテンツＤ１３の購入方法である。

【００５７】またサービス条件の再生可能回数とは、サービスプロバイダ３とユーザ宅９のユーザデバイス８とをオンライン接続し、サービスプロバイダ３からユーザデバイス８を介してユーザ記録メディア６にダウンロードしたディジタル音楽コンテンツＤ１３を、指定した再生可能回数の範囲内で再生し得るディジタル音楽コンテンツＤ１３の購入方法である。

【００５８】ポリシー記憶部２３は、コンテンツプロバイダセキュアコンテナＤ１４に含まれる取扱方針を記憶し、これをセキュアコンテナ作成部２５に送出する。

【００５９】セキュアコンテナ作成部２５は、図５に示すようにコンテンツキーKcoで暗号化されたディジタル音楽コンテンツＤ１３、配送用キーKd で暗号化されたコンテンツキーKco、取扱方針、価格情報及びディジタル署名を含むサービスプロバイダセキュアコンテナＤ２５を作成し、これを所定の通信インターフェース（図示せず）から専用のケーブルネットワーク、インターネット又は衛星放送等のネットワーク（図示せず）を介して決済端末５（図１）又はユーザ宅９のユーザデバイス８へオンラインで送信する。

【数７】

……（７）

【００５１】

【数８】

……（８）

【００６０】この場合のディジタル署名とは、コンテンツキーKcoで暗号化されたディジタル音楽コンテンツＤ１３、配送用キーKd で暗号化されたコンテンツキーKco、取扱方針、及び価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３における公開鍵暗号の秘密鍵Kssp で暗号化したデータである。

【００６１】相互認証部２４は、コンテンツプロバイダ２からコンテンツプロバイダセキュアコンテナＤ１４の供給を受けるのに先立って、ディジタル署名を用いてコンテンツプロバイダ２と相互認証する。また相互認証部２４は、決済端末５又はユーザデバイス８に対するサービスプロバイダセキュアコンテナＤ２５の送信に先立って、ディジタル署名を用いて決済端末５又はユーザデバイス８と相互認証する。

【００６２】従ってコンテンツサーバ２１は、相互認証部２４によってコンテンツプロバイダ２との間で相互認証が得られると、コンテンツプロバイダ２からコンテンツプロバイダセキュアコンテナＤ１４の供給を受け、セキュアコンテナ作成部２５は相互認証部２４によって決済端末５又はユーザデバイス８との間で相互認証が得られると、決済端末５又はユーザデバイス８に対してサービスプロバイダセキュアコンテナＤ２５を送信する。

【００６３】（１－３）決済端末の構成

決済端末５は、図６に示すようにサービスプロバイダ３（図１）や電子音楽配信センタ７（図１）とインターネット等のネットワークを介してデータ伝送を行う通信インターフェース３１と、当該通信インターフェース３１に接続されたＳＡＭ(Secure Application Module) ３２と、当該ＳＡＭ３２に接続されたハードディスクドライブ（ＨＤＤ）３３、液晶ディスプレイでなるモニタ３４及びフラッシュメモリカードでなるユーザ記録メディア６とデータ交換を行うためのフラッシュメモリカードインターフェース３５とから構成されている。

【００６４】ここでＳＡＭとは、電子音楽配信システム１の核をなすモジュールであり、決済処理、ディジタル音楽コンテンツの著作権管理処理、配送用キーKd の保持、コンテンツ再生履歴を表すユーザログの作成や削除等を実行するようになされており、決済端末５及びユーザ記録メディア６の記録再生機器であるユーザデバイス８（図１）にそれぞれ内蔵されている。

【００６５】決済端末５に内蔵されたＳＡＭ３２は、上述の機能に加えて電子音楽配信サービスセンタ７から伝

送された使用不許可ＳＡＭリスト（いわゆるブラックリスト）の保持、ディジタル音楽コンテンツの販売履歴の生成及び保持機能を有している。

【００６６】実際上ＳＡＭ３２は、動作する電圧又は周波数の幅が狭く外部からの不正なデータの読み出しが困難な（耐タンパー性）特性を持つシングルチップの暗号処理専用ＩＣ(Integrated Circuit)で構成され、相互認証モジュール４１、課金処理モジュール４２、記憶モジュール４３及び復号／暗号化モジュール４４を有している。なおユーザデバイス８においても、同様の構成のＳＡＭが内蔵されている。

【００６７】ＳＡＭ３２は、相互認証モジュール４１によってサービスプロバイダ３から送られるディジタル署名に基づいて相互認証を実行し、又は電子音楽配信サービスセンタ７との間で「Authentication and Key Exchange(AKE) Protocol using Asymmetric Key Algorithm」と呼ばれる非対称鍵暗号技術を用いた相互認証を実行する。

【００６８】非対称鍵暗号技術を用いた相互認証を実行するに当たって、例えば図７に示すように、決済端末５に内蔵されたＳＡＭ３２の相互認証モジュール４１は、

$$C1 = E_{...}\ （r1）$$

【００７２】に示すような暗号文Ｃ１を生成し、これを電子音楽配信サービスセンタ７へ通信インターフェース３１を介して送信する。

【００７３】電子音楽配信サービスセンタ７は、電子音楽配信サービスセンタ７の秘密鍵d_{esc}を用いた復号化

$$t1 = D_{...}\ （C1）$$

【００７５】に示すような平文ｔ１を求めた後、所定の乱数ｒ２を生成してＳＡＭ３２の公開鍵e_{sam}を用いた暗号化関数E_{sam}によって暗号化することにより、次式

$$C2 = E_{...}\ （r2）$$

【００７７】に示すような暗号文Ｃ２を生成し、当該暗号文Ｃ２と平文ｔ１とを決済端末５のＳＡＭ３２へ送信する。

【００７８】決済端末５のＳＡＭ３２は、相互認証モジュール４１によって乱数ｒ１と電子音楽配信サービスセンタ７から送られてきた平文ｔ１とが一致するか否かを検証し、一致したときには決済端末５が取り引きすべき

$$t2 = D_{...}\ （C2）$$

【００８０】に示すような平文ｔ２を求め、これを電子音楽配信サービスセンタ７へ送信する。

【００８１】電子音楽配信サービスセンタ７は、乱数ｒ２と決済端末５のＳＡＭ３２から送られてきた平文ｔ２とが一致するか否かを検証し、一致したときには電子音楽配信サービスセンタ７が取り引きすべき正当な決済端末５であることを認証し得、すなわち相互認証が完了する。

$$S = E_{...}\ （Ks）$$

予め電子音楽配信サービスセンタ７の公開鍵e_{esc}、ＳＡＭ３２の秘密鍵d_{sam}及びＳＡＭ３２の公開鍵e_{sam}を記憶しており、また電子音楽配信サービスセンタ７は当該電子音楽配信サービスセンタ７の公開鍵e_{esc}、電子音楽配信サービスセンタ７の秘密鍵d_{esc}、電子音楽配信サービスセンタ７に予め登録された決済端末５におけるＳＡＭ３２の公開鍵e_{sam}を予め記憶している。

【００６９】尚、ここではＳＡＭ３２の公開鍵e_{sam}を用いた暗号化関数をE_{sam}とし、ＳＡＭ３２の秘密鍵d_{sam}を用いた復号化関数をD_{sam}とする。また電子音楽配信サービスセンタ７の公開鍵e_{esc}を用いた暗号化関数をE_{esc}とし、電子音楽配信サービスセンタ７の秘密鍵d_{esc}を用いた復号化関数をD_{esc}とする。

【００７０】この場合決済端末５のＳＡＭ３２は、相互認証モジュール４１によって所定の乱数ｒ１を生成し、当該乱数ｒ１を電子音楽配信サービスセンタ７の公開鍵e_{esc}を用いた暗号化関数E_{esc}によって暗号化することにより、次式

【００７１】

【数９】

$$\cdots\cdots (9)$$

関数D_{esc}によって暗号文Ｃ１を復号することにより、次式

【００７４】

【数１０】

$$\cdots\cdots (10)$$

【００７６】

【数１１】

$$\cdots\cdots (11)$$

正当な電子音楽配信サービスセンタ７であることを認証し得、このときＳＡＭ３２の秘密鍵d_{sam}を用いた復号化関数D_{sam}によって暗号文Ｃ２を復号することにより、次式

【００７９】

【数１２】

$$\cdots\cdots (12)$$

【００８２】電子音楽配信サービスセンタ７は、相互認証が完了したので電子音楽配信サービスセンタ７と決済端末５との間で使用する共通鍵としてセッションキーＫｓを生成し、これをＳＡＭ３２の公開鍵e_{sam}を用いた暗号化関数E_{sam}によって暗号化することにより、次式

【００８３】

【数１３】

$$\cdots\cdots (13)$$

【００８４】に示すような暗号文Ｓを生成し、これを決済端末５のＳＡＭ３２へ送信する。

【００８５】決済端末５のＳＡＭ３２は、相互認証モジュール４１によって電子音楽配信サービスセンタ７から送られてきた暗号文ＳをＳＡＭ３２の秘密鍵d_{sam}を用

$$Ks = D_{...} \quad (S)$$

【００８７】に示すようなセッションキーKs を求める。

【００８８】これにより決済端末５は、以後電子音楽配信サービスセンタ７との間でデータ伝送を行う場合にセッションキーKs で暗号化するようになされている。これにより決済端末５と電子音楽配信サービスセンタ７との間で行われるデータ伝送のセキュリティを保証する。

【００８９】かくして電子音楽配信サービスセンタ７は、セッションキーKs に基づいて配送用キーKd 及び使用不許可ＳＡＭリスト（ブラックリスト）を暗号化して安全に決済端末５のＳＡＭ３２へデータ伝送し得るようになされている。

【００９０】決済端末５は、ＳＡＭ３２の相互認証モジュール４１によって電子音楽配信サービスセンタ７との相互認証が済むと、電子音楽配信サービスセンタ７から送られてきた配送用キーKd 及び使用不許可ＳＡＭリストをＳＡＭ３２の記憶モジュール４３に記憶する。

【００９１】また決済端末５は、ＳＡＭ３２の相互認証モジュール４１によってサービスプロバイダ３との相互認証が済むと、通信インターフェース３１を介してサービスプロバイダ３からサービスプロバイダセキュアコンテナＤ２５を取り込み、そのうちの取扱情報及び価格情報に基づいてサービス条件情報及び課金情報を生成し、これらを記憶モジュール４３に格納する。

【００９２】このとき同時に決済端末５は、サービスプロバイダセキュアコンテナＤ２５のうちコンテンツキーKcoによって暗号化されたディジタル音楽コンテンツＤ１３をハードディスクドライブ３３に格納する。なお、このディジタル音楽コンテンツＤ１３のコンテンツキーKcoは、配送用キーKd によって暗号化された状態である。

【００９３】そして決済端末５は、ユーザによって持ち込まれたユーザ記録メディア６がカードスロット５０Ａを介して装着されて読取手段としてのフラッシュメモリカードインターフェース５０に接続されると、当該フラッシュメモリカードインターフェース５０によってユーザ記録メディア６の所定記憶領域に格納されている公開鍵証明書を読み出し、これを記憶モジュール４３に格納する。

【００９４】ここで公開鍵証明書とは、電子音楽配信サービスセンタ７から発行されたデータで、ユーザデバイス８の出荷時に内蔵されたＳＡＭに予め保持されており、ＳＡＭ公開鍵Kpub とＳＡＭのＩＤ(IDentification)番号であるＳＡＭＩＤとを含み、ユーザデバイス８に

いた復号化関数D_{sam}を用いて復号することにより、次式

【００８６】

【数１４】

$$\cdots\cdots (14)$$

よってユーザ記録メディア６の所定記憶領域に記録されている。

【００９５】決済端末５は、記憶モジュール４３に格納されたＳＡＭ公開鍵Kpub を読み出して通信インターフェース３１を介して電子音楽配信サービスセンタ７へ送信する。

【００９６】電子音楽配信サービスセンタ７は、ＳＡＭ公開鍵Kpub に基づいてユーザデバイス８が電子音楽配信サービスセンタ７に予め登録されたものであることを判別し、この結果を決済端末５へ通知する。

【００９７】決済端末５は、電子音楽配信サービスセンタ７からユーザデバイス８が正規ユーザのものであることを通知してもらうと、認証手段としての相互認証モジュール４２により記憶モジュール４３に格納されているＳＡＭＩＤと使用不許可ＳＡＭリスト（ブラックリスト）とを比較して、ＳＡＭＩＤが使用不許可ＳＡＭリストに記載されているか否かを判別する。

【００９８】ここで決済端末５は、相互認証モジュール４２によりユーザデバイス８が正規ユーザのものであり、かつブラックリストに記載されていないことを認識すると、ＧＵＩ(Graphical User Interface)生成モジュール５１にＧＵＩ画面の生成を指示する。

【００９９】ＧＵＩ生成モジュール５１は、記憶モジュール４３から読み出したサービス条件情報及び課金情報に基づいてディジタル音楽コンテンツの曲名を表したＧＵＩ画面及び買い切りの対価を表したＧＵＩ画面を生成し、これらをモニタ３４に表示する。

【０１００】ＧＵＩ生成モジュール５１は、モニタ３４に表示されたＧＵＩ画面上でユーザによりディジタル音楽コンテンツが選択され、当該選択されたディジタル音楽コンテンツの対価が所定の現金投入口やカード投入口を介して現金、プリペイドカード又はキャッシュカード等のいずれかによって支払われたことを確認すると、その旨を決済手段としての課金処理モジュール４２に通知する。

【０１０１】課金処理モジュール４２は、選択されたディジタル音楽コンテンツにおける買い切りの対価の支払いによりディジタル音楽コンテンツの決済を行って決済処理が終了すると、その旨を復号／暗号化モジュール４４に対して通知する。

【０１０２】復号／暗号化モジュール４４は、復号ユニット４５、暗号化ユニット４６及び記録ユニット４７によって構成され、決済終了の通知を課金処理モジュール４２から受けると、復号ユニット４５によってハードデ

ィスクドライブ３３からコンテンツキーKcoで暗号化されたディジタル音楽コンテンツＤ１３を読み出すと共に、記憶モジュール４３から読み出した配送用キーKd でディジタル音楽コンテンツＤ１３のコンテンツキーKcoを復号して暗号化ユニット４７に送出する。

【０１０３】暗号化ユニット４７は、配送用キーKd で復号されたコンテンツキーKcoを記憶モジュール４３から読み出した公開鍵証明書のＳＡＭ公開鍵Kpub で再度暗号化し、当該ＳＡＭ公開鍵Kpub で暗号化されたコンテンツキーKcoとコンテンツキーKcoで暗号化されたディジタル音楽コンテンツＤ１３とを、データ記録手段としての記録ユニット４８によってフラッシュメモリカードインターフェース５０を介してユーザ記録メディア６に書き込むと共に、書き込み終了したことをＧＵＩ生成モジュール５１に通知する。

【０１０４】ＧＵＩ生成モジュール５１は、コンテンツキーKcoで暗号化されたディジタル音楽コンテンツＤ１３及びＳＡＭ公開鍵Kpub で暗号化されたコンテンツキーKcoのユーザ記録メディア６に対する書き込みが終了した旨を表したＧＵＩ画面を生成し、これをモニタ３４に表示してユーザへ通知する。これにより決済端末５は、買い取りで購入されたディジタル音楽コンテンツのユーザ記録メディア６に対する書き込み及びその決済を終了する。

【０１０５】この結果、ユーザ記録メディア６にはコンテンツキーKcoで暗号化されたディジタル音楽コンテンツＤ１３と、ＳＡＭ公開鍵Kpub によって暗号化されたコンテンツキーKcoとが記録される。

【０１０６】ユーザ宅９に設置されたユーザデバイス８は、ディジタル音楽コンテンツの記録されたユーザ記録メディア６が装填されると、内蔵されたＳＡＭによりＳＡＭ公開鍵Kpub に対応したＳＡＭ秘密鍵でコンテンツキーKcoを復号し、当該復号したコンテンツキーKcoでディジタル音楽コンテンツＤ１３を復号することにより再生データを生成し、これをスピーカ（図示せず）を介して出力する。

【０１０７】ところで復号ユニット４５は、ユーザによって選定されたディジタル音楽コンテンツＤ１３のコンテンツキーKcoを配送用キーKd で復号したときには、その旨を課金処理モジュール４２に通知する。

【０１０８】このとき課金処理モジュール４２は、配送用キーKd でコンテンツキーKcoを復号した旨の通知を受ける度にコンテンツ再生履歴を表すユーザログを生成すると共に、買い取りで購入されたディジタル音楽コンテンツＤ１３の販売履歴（顧客情報やディジタル音楽コンテンツの種類を表すコンテンツ情報）を生成して記憶モジュール４３に保存する。

【０１０９】そして決済端末５は、相互認証モジュール４１により電子音楽配信サービスセンタ７との間で非対称鍵暗号技術を用いて相互認証を行った後に、課金処理モジュール４２により記憶モジュール４３からユーザログ及び販売履歴を読み出し、当該ユーザログ及び販売履歴をセッションキーKs で暗号化した後に送信手段としての通信インターフェース３１を介して電子音楽配信サービスセンタ７へ送信する。

【０１１０】かくして電子音楽配信サービスセンタ７は、決済端末５から送られてきたユーザログ及び販売履歴に基づいてディジタル音楽コンテンツの再生履歴や、ユーザのディジタル音楽コンテンツの販売状況を調査し得るようになされている。

【０１１１】（２）買い取りでディジタル音楽コンテンツをオフライン購入するときの決済シーケンス

続いて、電子音楽配信システム１において買い取りでディジタル音楽コンテンツをオフライン購入するときの決済シーケンスについて、図８を用いて説明する。

【０１１２】まず第１ステップ（ＳＰ）として、決済端末５は電子音楽配信サービスセンタ７との間で非対称鍵暗号技術を用いた相互認証（図７）を実行し、電子音楽配信サービスセンタ７からセッションキーKs で暗号化された配送用キーKd 及び使用不許可ＳＡＭリスト（ブラックリスト）の供給を受ける。

【０１１３】第２ステップとして、決済端末５は、サービスプロバイダ３との間でディジタル署名を用いて相互認証を実行した後、サービスプロバイダ３からサービスプロバイダセキュアコンテナＤ２５の供給を受け、そのうちコンテンツキーKcoで暗号化されたディジタル音楽コンテンツＤ１３と、配送用キーKd で暗号化されたコンテンツキーKcoをハードディスクドライブ３３に格納する。

【０１１４】第３ステップとして、決済端末５はユーザによってカードスロット５０Ａにユーザ記録メディア６が装着され、フラッシュメモリカードインターフェース５０を介してユーザ記録メディア６の所定記憶領域から公開鍵証明書のＳＡＭ公開鍵Kpub 及びＳＡＭＩＤを読み出してＳＡＭ３２の記憶モジュール４３に格納する。

【０１１５】第４ステップとして、決済端末５はＳＡＭ公開鍵Kpub に基づいてユーザデバイス８が正規ユーザであることを電子音楽配信サービスセンタ７から通知された後、ＳＡＭＩＤに基づいてブラックリストに記載されたユーザでないことを確認すると、モニタ３４にディジタル音楽コンテンツの曲名を表したＧＵＩ画面を表示する。

【０１１６】第５ステップとして、決済端末５はＧＵＩ画面上におけるユーザ操作によって選定されたディジタル音楽コンテンツを判別し、第６ステップとして、選定されたディジタル音楽コンテンツの利用料金を表したＧＵＩ画面をモニタ３４に表示する。

【０１１７】第７ステップとして、決済端末５はモニタ３４のＧＵＩ画面上に表示された利用料金の入金処理がユーザによって完了したことをＳＡＭ３２の課金処理モ

ジュール４２によって確認する。

【０１１８】第８ステップとして、決済端末５は復号／暗号化モジュール４４によってディジタル音楽コンテンツＤ１３のコンテンツキーKcoを配送用キーKd で復号し、当該復号したコンテンツキーKcoをＳＡＭ公開鍵Kpub で再度暗号化し、当該ＳＡＭ公開鍵Kpub で暗号化されたコンテンツキーKcoと、コンテンツキーKcoで暗号化されたディジタル音楽コンテンツＤ１３とをユーザ記録メディア６に書き込む。

【０１１９】第９ステップとして、決済端末５は復号／暗号化モジュール４４によって配送用キーKd でコンテンツキーKcoを復号したときに課金処理モジュール４２によってユーザログを生成すると共に、買い取り購入されたディジタル音楽コンテンツＤ１３の販売履歴（顧客情報やディジタル音楽コンテンツの種類を表すコンテンツ情報）を生成して記憶モジュール４３に保存する。

【０１２０】第１０ステップとして、決済端末５は相互認証モジュール４１により電子音楽配信サービスセンタ７との間で相互認証を行った後、第１１に、課金処理モジュール４２により記憶モジュール４３からユーザログ及び販売履歴を読み出し、当該販売履歴をセッションキーKs で暗号化した後に通信インターフェース３１を介して電子音楽配信サービスセンタ７へ送信する。

【０１２１】（３）ディジダル音楽コンテンツをオンライン購入するときのユーザログを用いた決済シーケンス次に、電子音楽配信システム１（図１）においてサービスプロバイダ３とユーザ宅９のユーザデバイス８とがインターネット等のネットワークを介してオンライン接続された状態で、サービスプロバイダ３に対して所望のディジタル音楽コンテンツを指定し、サービスプロバイダ３から供給される所望のディジタル音楽コンテンツをユーザデバイス８を介してユーザ記録メディア６に書き込み、当該ユーザ記録メディア６に書き込まれたディジダル音楽コンテンツを再生したときに再生回数分の利用料金を支払う決済シーケンスを、図９を用いて説明する。

【０１２２】ここでユーザ記録メディア６には、ユーザデバイス８の内蔵ＳＡＭによってディジダル音楽コンテンツの再生回数に応じたユーザログが所定記憶領域に記録され、かくして決済端末５はユーザ記録メディア６からユーザログを読み出し、当該読み出したユーザログに基づいて利用料金を決済するようになされている。

【０１２３】まず第１ステップ（ＳＰ）として、決済端末５はユーザによって持参されたユーザ記録メディア６がカードスロット５０Ａに装着されることにより、ユーザ記録メディア６の所定記憶領域に記録されたユーザログ及び公開鍵証明書を読み出す。なおユーザログは、楕円曲線暗号によってディジタル署名されており、改ざんされないように暗号化されている。

【０１２４】第２ステップとして、決済端末５は電子音楽配信サービスセンタ７との間で非対称鍵暗号技術を用いた相互認証を実行し、電子音楽配信サービスセンタ７からセッションキーKs で暗号化された配送用キーKd 及び使用不許可ＳＡＭリスト（ブラックリスト）の供給を受ける。

【０１２５】このとき決済端末５は、公開鍵証明書に含まれているＳＡＭ公開鍵Kpub に基づいてユーザデバイス８が正規ユーザのものであることを電子音楽配信サービスセンタ７から通知され、公開鍵証明書に含まれているＳＡＭＩＤに基づいて使用不許可ＳＡＭリストに記載されたユーザではないことを確認すると、ユーザログを読み取ると共に当該ユーザログを読み取ったことを表す確認フラグを立てる。これによりユーザ記録メディア６には、確認フラグが立てられたので、決済端末５のカードスロット５０Ａに再度装着されたときにユーザログが再度読み取られることがなく、利用料金の支払い請求を２度受けずに済む。

【０１２６】第３ステップとして、決済端末５はユーザ記録メディア６から読み出したユーザログ及び公開鍵証明書を電子音楽配信サービスセンタ７に対してインターネット等のネットワークを介して送信する。これにより電子音楽配信サービスセンタ７は、ユーザログに基づいて再生回数に応じた利用料金を算出し、ユーザに対する請求金額情報をネットワークを介して決済端末５へ送信する。

【０１２７】第４ステップとして、決済端末５は電子音楽配信サービスセンタ７から送られてきた利用料金の請求金額情報を受信し、ＧＵＩ生成モジュール５１によって請求金額情報に基づく利用料金を表したＧＵＩ画面を生成する。

【０１２８】第５ステップとして、決済端末５は請求金額情報に基づく利用料金を表したＧＵＩ画面をモニタ３４に表示してユーザに通知する。ユーザは、モニタ３４に表示されたＧＵＩ画面を確認することにより、再生回数に応じた利用料金の金額を認識し得る。

【０１２９】第６ステップとして、決済端末５はユーザによって利用料金の入金処理が完了したことを確認すると、第７ステップとして課金処理モジュール４２により入金処理完了情報を通信インターフェース３１を介して電子音楽配信サービスセンタ７へ送信する。

【０１３０】電子音楽配信サービスセンタ７は、入金処理完了情報を受け取るとユーザログに基づく再生回数に応じた利用料金の決済が終了したので、公開鍵証明書のＳＡＭ公開鍵Kpub で暗号化したユーザログ削除許可証を生成し、これを決済端末５へ送信する。

【０１３１】第８ステップとして、決済端末５は電子音楽配信サービスセンタ７からＳＡＭ公開鍵Kpub で暗号化されたユーザログ削除許可証を受信する。第９に、決済端末５は電子音楽配信サービスセンタ７から受信したユーザログ削除許可証をＳＡＭ公開鍵Kpub に対応したＳＡＭ秘密鍵で復号して、当該復号したユーザログ削除

許可証に基づいてユーザログを削除する。

【０１３２】ここで決済端末５は、ユーザログ削除許可証に基づいてユーザログを削除する場合、確認フラグが立っていることを確認したときにユーザログを削除するようになされている。これによりユーザ記録メディア６は、所定記憶領域に記録されたユーザログが削除され、再生回数分の利用料金の決済が全て終了する。

【０１３３】（４）実施の形態における動作及び効果

以上の構成において、電子音楽配信システム１の店舗４に設置されている決済端末５は、ユーザが買い取りでディジタル音楽コンテンツをオフライン購入する場合、まず電子音楽配信サービスセンタ７との間で相互認証を実行した後に配送用キーKd 及び使用不許可ＳＡＭリストの供給を受ける。

【０１３４】次に決済端末５は、サービスプロバイダ３との間で相互認証を実行した後にサービスプロバイダ３から供給されるコンテンツキーKcoで暗号化されたディジタル音楽コンテンツＤ１３と、配送用キーKd で暗号化されたコンテンツキーKcoとをハードディスクドライブ３３に予め記憶しておく。

【０１３５】ユーザデバイス８は、内蔵ＳＡＭによってユーザ記録メディア６の所定記憶領域に公開鍵証明書を記録し、ユーザは公開鍵証明書の記録されたユーザ記録メディア６を持参して店舗５に設置された決済端末５のカードスロット５０Ａにユーザ記録メディア６を装着する。

【０１３６】そして決済端末５は、ユーザによってカードスロット５０Ａに装着されたユーザ記録メディア６から公開鍵証明書のＳＡＭ公開鍵Kpub 及びＳＡＭＩＤを読み出し、ユーザデバイス８がブラックリストに記載されていない正規ユーザであることを確認すると、ディジタル音楽コンテンツの曲名及び買い切りの対価を表したＧＵＩ画面をモニタ３４に表示する。

【０１３７】続いて決済端末５は、ユーザによってディジタル音楽コンテンツの曲名が選定され、その利用料金の入金処理が完了したことを確認すると、配送用キーＫd でコンテンツキーKcoを復号すると共にユーザログを生成し、ＳＡＭ公開鍵Kpubでコンテンツキーkcoを再度暗号化した後、当該ＳＡＭ公開鍵Kpub で再度暗号化されたコンテンツキーKcoと、コンテンツキーKcoで暗号化されているディジタル音楽コンテンツＤ１３とをユーザ記録メディア６に書き込む。

【０１３８】最後に決済端末５は、生成したユーザログと共にディジタル音楽コンテンツの販売履歴を電子音楽配信サービスセンタ７へ送信し、ディジタル音楽コンテンツをオフライン購入したときの決済処理を終了する。

【０１３９】また決済端末５は、ユーザがディジダル音楽コンテンツをサービスプロバイダ３からオンライン購入する場合、ユーザによって持参されたユーザ記録メディア６がカードスロット５０Ａに装填されると、ユーザ記録メディア６から再生回数に応じて記録されたユーザログ及び公開鍵証明書を読み出し、そのうちの公開鍵証明書に基づいてユーザデバイス８が正規ユーザのものであることを確認する。

【０１４０】そして決済端末５は、記録メディア６から読み出したユーザログ及び公開鍵証明書を電子音楽配信サービスセンタ７に対してインターネット等のネットワークを介して送信する。これにより電子音楽配信サービスセンタ７は、ユーザログに基づいて再生回数に応じた利用料金を算出し、ユーザに対する請求金額情報をネットワークを介して決済端末５へ送信する。

【０１４１】続いて決済端末５は、電子音楽配信サービスセンタ７から送られてきた利用料金の請求金額情報に基づく利用料金を表したＧＵＩ画面をモニタ３４に表示し、ユーザによって利用料金の入金処理が完了したことを確認すると、入金処理完了情報を電子音楽配信サービスセンタ７へ送信する。

【０１４２】これにより電子音楽配信サービスセンタ７は、入金処理完了情報を受け取るとユーザ記録メディア６に記録されたユーザログの決済が終了したので、公開鍵証明書のＳＡＭ公開鍵Kpub で暗号化したユーザログ削除許可証を決済端末５へ送信する。

【０１４３】最後に決済端末５は、電子音楽配信サービスセンタ７から送られてきたユーザログ削除許可証をＳＡＭ秘密鍵で復号し、当該復号したユーザログ削除許可証に基づいてユーザログを削除した後にユーザ記録メディア６をユーザへ返却し、ディジタル音楽コンテンツをサービスプロバイダ３からオンライン購入したときの決済処理を終了する。

【０１４４】このように決済端末５は、ディジタル音楽コンテンツをオフライン購入又はオンライン購入する場合においても、ユーザ記録メディア６から公開鍵証明書のＳＡＭ公開鍵Kpub 及びＳＡＭＩＤを読み出し、当該ＳＡＭ公開鍵Kpub 及びＳＡＭＩＤに基づいてユーザデバイス８を認証する。

【０１４５】そして決済端末５は、ユーザデバイス８が正規ユーザのものであることを確認した場合にだけ、ユーザによって選定されたディジタル音楽コンテンツをユーザ記録メディア６に書き込むことにより、ＳＡＭ内蔵のユーザデバイス８を所有している正規ユーザに対してのみディジタル音楽コンテンツを供給することができる。

【０１４６】同時に決済端末５は、ディジタル音楽コンテンツを供給する際にユーザデバイス８毎に設定されたＳＡＭ公開鍵Kpub でコンテンツキーKcoをさらに暗号化しているので、ＳＡＭ公開鍵Kpub に対応したＳＡＭ秘密鍵を保持するＳＡＭ内蔵のユーザデバイス８によってのみコンテンツキーKcoを復号してディジタル音楽コンテンツを再生することができる。

【０１４７】すなわち電子音楽配信システム１では、デ

ィジタル音楽コンテンツの記録されたユーザ記録メディア６を他人の所有するユーザデバイスで再生することはできず、かくしてディジタル音楽コンテンツの著作権を有益に保護することができる。

【０１４８】また決済端末５は、ユーザデバイス８が正規ユーザのものであることを確認したときにディジタル音楽コンテンツの買い切りの対価又は再生回数に応じた利用料金を表したＧＵＩ画面をモニタ３４に表示し、ユーザによって現金、プリペイドカード又はキャッシュカード等のいずれかによって入金処理が実行されるようになされており、これにより、ユーザに対して自分自身を証明するクレジット番号等を入力する等の煩雑な手続きを強いることなく決済を完了することができる。

【０１４９】かくして電子音楽配信システム１では、サービスプロバイダ３とオンライン接続し得るユーザデバイス８を所有しないユーザであっても、ＳＡＭを内蔵したポータブル機器やカーオーディオ等を所有してさえいれば、店舗４に設置されている決済端末５を介して所望のディジタル音楽コンテンツをオフライン購入し得ると共に、その場で現金、プリペイドカード又はキャッシュカード等のいずれかによって容易に決済することができる。

【０１５０】またユーザは、ユーザデバイス８とサービスプロバイダ３とをオンライン接続して所望のディジタル音楽コンテンツをオンライン購入した場合でも、内蔵ＳＡＭによってユーザログの記録されたユーザ記録メディア６を店舗４へ持参して決済端末５へ装着し、当該決済端末５によって指示された再生回数に応じた利用料金をその場で容易に決済することができる。

【０１５１】かくしてユーザは、電子音楽配信サービスセンタ７に対して自分自信を証明するクレジットカード番号等をオンラインで送信する必要がないので面倒な手続きなしに決済することができる。

【０１５２】さらに決済端末５では、サービスプロバイダ３から予めディジタル音楽コンテンツをダウンロードしてハードディスクドライブ３３に格納しておくことにより、オフライン購入する場合にユーザ記録メディア６に対してダウンロードに要する時間が不要になり、決済端末５のデータ転送速度でユーザ記録メディア６にディジタル音楽コンテンツを書き込むことができ、かくして買い取りでオフライン購入するユーザに対して購入時の待ち時間を大幅に短縮することができる。

【０１５３】さらに電子音楽配信システム１は、ユーザログと共に販売履歴を決済端末５から電子音楽配信サービスセンタ７へ送信するようにしたことにより、当該電子音楽配信サービスセンタ７によってディジタル音楽コンテンツのマーケティングリサーチを容易に実行することができる。

【０１５４】以上の構成によれば、電子音楽配信システム１はディジタル音楽コンテンツをオンライン購入又はオフライン購入する場合、ユーザ記録メディア６から読み出した公開鍵証明書に基づいてユーザデバイス８が正規ユーザのものであることを確認したとき、オフライン又はオンラインによるディジタル音楽コンテンツの供給条件に対応した対価の入金を受けて決済するようにしたことにより、自分自信を証明するクレジットカード番号等の面倒な入力手続きを正規ユーザに対して強いることなく容易に決済することができる。

【０１５５】（５）他の実施の形態

なお上述の実施の形態においては、提供データとしてディジタル音楽コンテンツを提供するようにした場合について述べたが、本発明はこれに限らず、映画やゲーム又はアプリケーションソフトウェア等の種々のディジタルデータを提供するようにしても良い。この場合にも、上述の実施の形態と同様の効果を得ることができる。

【０１５６】また上述の実施の形態においては、電子音楽配信サービスセンタ７とコンテンツプロバイダ２、コンテンツプロバイダ２とサービスプロバイダ３、サービスプロバイダ３と決済端末５との間をオンライン接続してデータ伝送するようにした場合について述べたが、本発明はこれに限らず、オフラインでデータを供給するようにしても良い。

【０１５７】さらに上述の実施の形態においては、ユーザがディジタル音楽コンテンツを買い取りでオフライン購入するようにした場合について述べたが、本発明はこれに限らず、オフラインで指定した再生可能回数でディジタル音楽コンテンツを購入し、再生回数に応じて記録されたユーザログに基づいて決済端末５で決済するようにしても良い。この場合、ユーザ記録メディア６にディジタル音楽コンテンツを記録するときに決済を行うのではなく、ユーザデバイス８によってユーザ記録メディア６に記録されたユーザログを決済端末５に再度読み取らせることにより決済を行う。

【０１５８】さらに上述の実施の形態においては、記録媒体であるユーザ記録メディア６としてフラッシュメモリカードを記録媒体として用いるようにした場合について述べたが、本発明はこれに限らず、光磁気ディスク等の他の種々の記録媒体を用いるようにしても良い。

【０１５９】さらに上述の実施の形態においては、ユーザがディジタル音楽コンテンツをサービスプロバイダ３からオンライン購入したとき、ユーザデバイス８によって再生回数に応じたユーザログをユーザ記録メディア６に記録し、当該ユーザ記録メディア６を介して決済端末５に直接ユーザログを読み取らせ、当該決済端末５から電子音楽配信サービスセンタ７へユーザログを送信するようにした場合について述べたが、本発明はこれに限らず、ユーザデバイス８の内蔵ＳＡＭが生成したユーザログをサービスプロバイダ３へオンラインで直接送信するようにしても良い。この場合、ユーザデバイス８はユーザログを送信し終わったことを示す確認フラグを立て、

再度送信することを防止する。

【０１６０】さらに上述の実施の形態においては、決済端末５がモニタ３４にディジタル音楽コンテンツの曲名や利用料金だけを表示するようにした場合について述べたが、本発明はこれに限らず、曲名のラベルプリント機能や、ディジタル音楽コンテンツの試聴機能、さらにアーティストの顔写真を表示した静止画像をモニタ３４に表示する表示機能等の種々の付加機能を設定するようにしても良い。

【０１６１】

【発明の効果】上述のように本発明によれば、記録媒体から読み取ったユーザ識別情報を基にユーザ機器を認証し得た場合に限って、ユーザに選択された提供データの供給条件に対応した対価の入金を受け付けて決済を行うようにしたことにより、認証し得た特定のユーザに対して支払いを行うための個人データの煩雑な入力手続きを強いることなく提供データの決済を行うことができ、かくして供給される提供データの決済を煩雑な手続きなしに容易に実行し得るデータ決済装置及びデータ決済方法を実現できる。

【０１６２】また本発明によれば、記録媒体から読み取ったユーザ識別情報を基にユーザ機器を認証し得た場合に限って、データ配信装置から配信されてユーザに選択された提供データの供給条件に対応した対価の入金を受け付けて決済を行うようにしたことにより、認証し得た特定のユーザに対して支払いを行うための個人データの煩雑な入力手続きを強いることなく提供データの決済を行うことができ、かくして供給される提供データの決済をデータ決済装置によって煩雑な手続きなしに容易に実行し得るデータ決済システムを実現できる。

【図面の簡単な説明】

【図１】本発明による電子音楽配信システムの全体構成を示すブロツク図である。

【図２】コンテンツプロバイダの構成を示すブロツク図である。

【図３】コンテンツプロバイダセキュアコンテナのデータ構造を示す略線図である。

【図４】サービスプロバイダの構成を示すブロツク図である。

【図５】サービスプロバイダセキュアコンテナのデータ構造を示す略線図である。

【図６】決済端末の構成を示すブロツク図である。

【図７】決済端末と電子音楽配信サービスセンタとの間における相互認証の処理シーケンスを示す略線図である。

【図８】買い取りでディジタル音楽コンテンツをオフライン購入するときの決済シーケンスを示す略線図である。

【図９】ディジタル音楽コンテンツをオンライン購入するときのユーザログを用いた決済シーケンスを示す略線図である。

【符号の説明】

１……電子音楽配信システム、２……コンテンツプロバイダ、３……サービスプロバイダ、５……決済端末、６……ユーザ記録メディア、７……電子音楽配信サービスセンタ、８……ユーザデバイス、３２……ＳＡＭ、３３……ＨＤＤ、３４……モニタ、４１……相互認証モジュール、４２……課金処理モジュール、４３……記憶モジュール、４４……復号／暗号化モジュール、４５……復号ユニット、４６……暗号化ユニット、４７……記録ユニット、５０……フラッシュメモリカードインターフェース、５１……ＧＵＩ生成モジュール。

【図１】

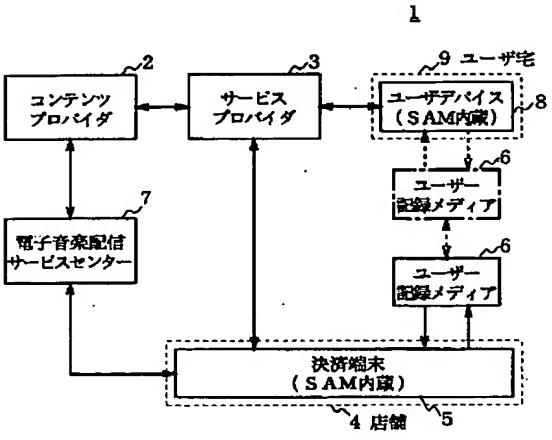


図１　電子音楽配信システムの全体構成

【図４】

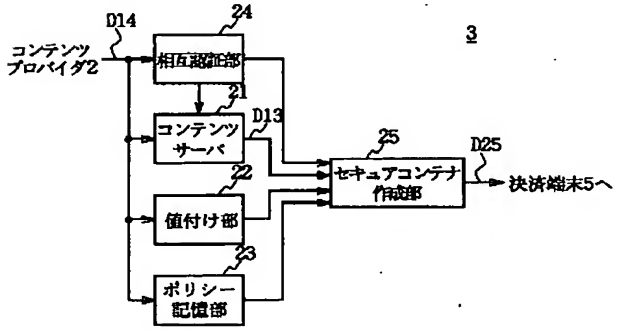


図４　サービスプロバイダの構成

【図２】

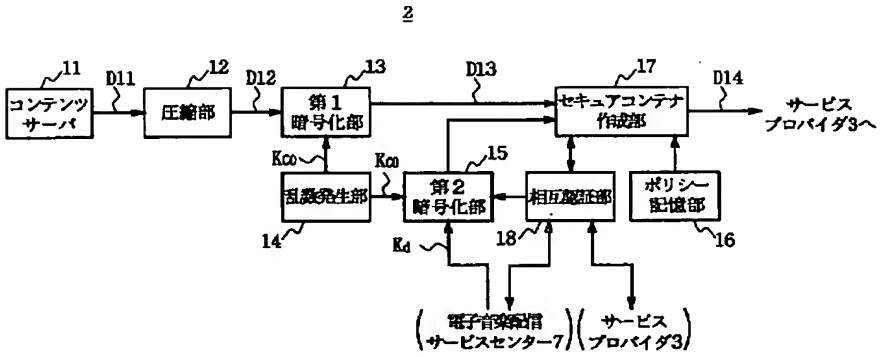


図２　コンテンツプロバイダの構成

【図３】

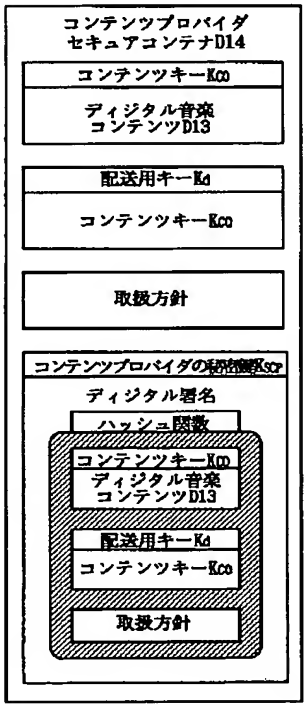


図３　コンテンツプロバイダセキュアコンテナのデータ構造

【図５】

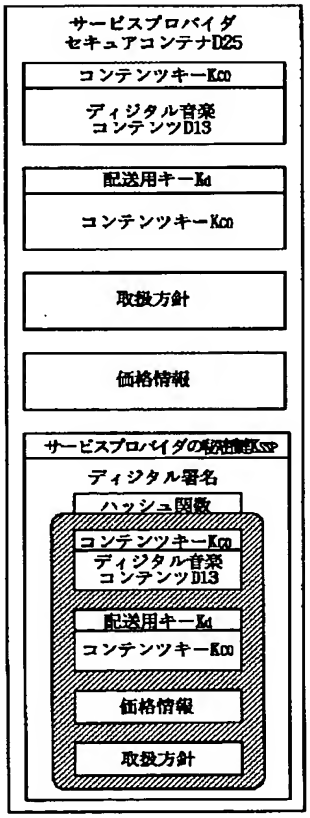


図５　サービスプロバイダセキュアコンテナのデータ構造

【図６】

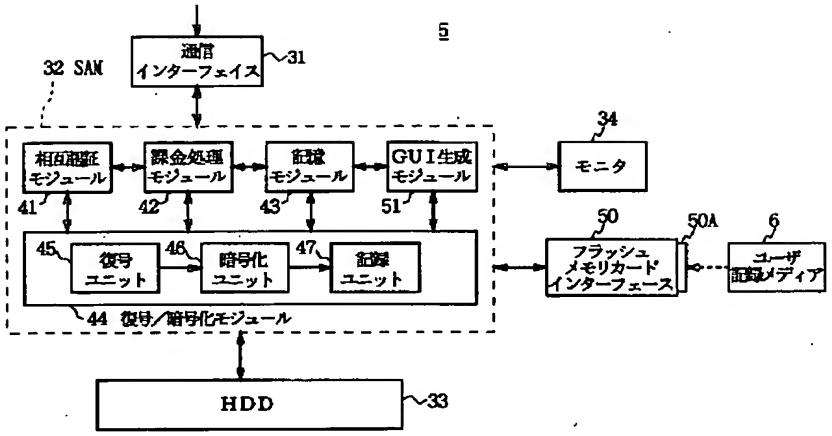


図６　決済端末の構成

【図７】

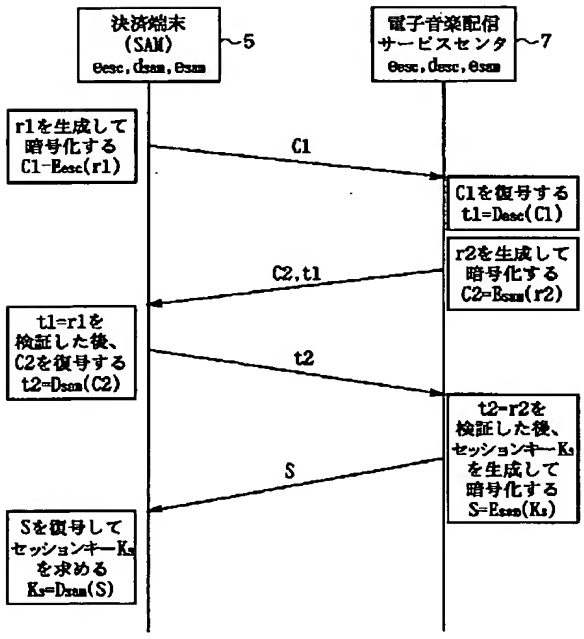


図７　決済端末と電子音楽配信サービスセンタとの間における相互認証の処理シーケンス

【図８】

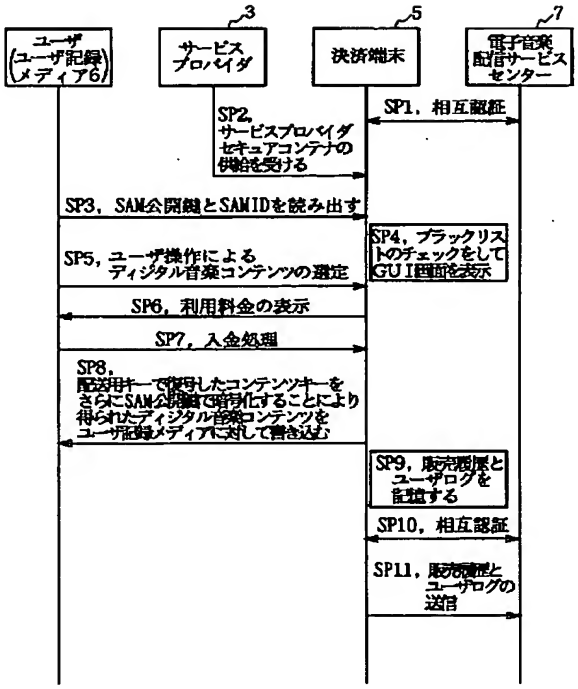


図８　買い取りでディジタル音楽コンテンツをオフライン購入するときの決済シーケンス

【図９】

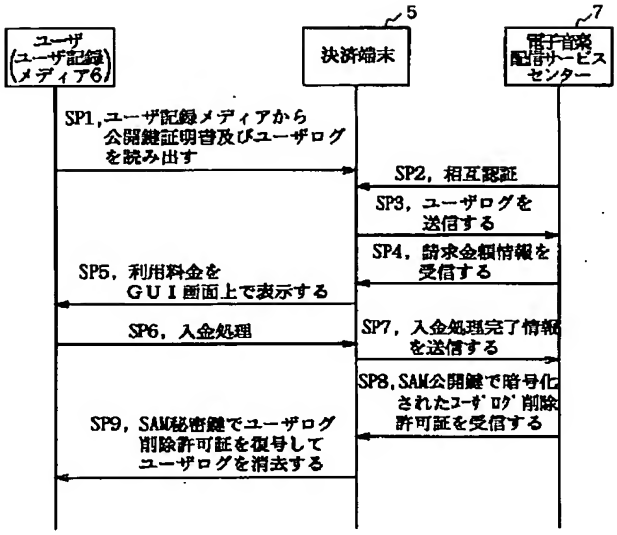


図９　ディジタル音楽コンテンツをオンライン購入するときのユーザログを用いた決済シーケンス

フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
		Ｈ０４Ｌ	9/00	６７３Ｂ
		Ｇ０６Ｆ	15/30	Ｌ

Ｆターム(参考) 5B049 AA05 BB11 CC05 CC36 DD05
EE03 FF02 FF03 FF04 FF06
FF08 FF09 GG04 GG07 GG10
5B055 BB11 CB09 EE02 EE04 EE17
EE27 LL07 PA02 PA34 PA38
5D044 AB03 BC01 CC04 DE49 EF05
FG18 GK17 HL02
5J104 AA07 KA01 KA15 MA02 NA38
PA07 PA10